Kongruenzrechnung

Def.: Sei $n \in \mathbb{N}$, und seien $a, b \in \mathbb{Z}$.

$$a \equiv b \bmod n \iff n \mid b - a$$
$$\iff \exists k \in \mathbb{Z} : b - a = kn$$

Eigenschaften der Kongruenzrelation:

i) ist eine Äquivalenzrelation (reflexiv, symmetrisch und transitiv) Auf Grund der Transitivität lassen sich Kongruenzen verketten Sind $a_1, a_2, \ldots, a_m \in \mathbb{Z}$, dann

der Transitivität lassen sich Kongruenzen

schreibt man statt $a_1 \equiv a_2 \bmod n$, $a_2 \equiv a_3 \bmod n$, $\dots$, $a_{m-1} \equiv a_m \bmod n$ auch einfach

$$a_1 \equiv a_2 \equiv \dots \equiv a_{m-1} \equiv a_m \bmod n.$$

Es gilt $a_1 \equiv a_m \bmod n$.

Seien $a, b, c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$.

(iii) $a \equiv b \bmod m$, $c \equiv d \bmod m \Rightarrow$
$a+c \equiv b+d \bmod m$, $ac \equiv bd \bmod m$.

(iii) $a \equiv b \bmod n$, $m \mid n \Rightarrow a \equiv b \bmod m$

(iv) $a \equiv b \bmod n \iff ma \equiv mb \bmod mn$

(v) $a \equiv b \bmod n \iff a + n\mathbb{Z} = b + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$

(vi) Der Chinesische Restsatz für den Ring $\mathbb{Z}$ ist gleichwertig mit folgender Aussage: Sind $m_1, \dots, m_r \in \mathbb{N}$ paarweise teilerfremd ($r \geq 2$) und sind $a_1, \dots, a_r \in \mathbb{Z}$ bel. vorgeg., dann existiert eine Lösung $a \in \mathbb{Z}$ des Kongruenzsystems $x \equiv a_1 \bmod m_1, \dots, x \equiv a_r \bmod m_r$.

Ist $b \in \mathbb{Z}$ eine weitere Lösung, dann gilt $a \equiv b \bmod m$, wobei $m = m_1 \cdot \dots \cdot m_r$.

Frage: Lassen sich auch Kongruenzsysteme zu nicht paarweise teilerfremden m_i lösen, z.B.

$x \equiv a \bmod 33$, $x \equiv b \bmod 39$, mit $a, b \in \mathbb{Z}$?

Frage: Lassen sich auch Kongruenzsysteme zu nicht paarweise teilerfremden m lösen → R

- Das System ist genau dann lösbar, wenn $a \equiv b \bmod 3$ erfüllt ist
- Sei $c \in \{0, 1, 2\}$ der eindeutig bestimmte Repräsentant von dieser Restklasse
  $\Rightarrow \exists k, l \in \mathbb{Z}$ mit $a = c + 3k$, $b = c + 3l$
- Jede Lösung hat die Form $c + 3y$ mit $y \in \mathbb{Z}$.

einsetzen einsetzen $\Rightarrow c + 3y \equiv c + 3k \bmod 33$

$\wedge\ c + 3y \equiv c + 3l \bmod 39$ ⇝

$3y \equiv 3k \bmod 33 \wedge 3y \equiv 3l \bmod 39$ ⇜

$y \equiv k \bmod 11 \wedge y \equiv l \bmod 13$

n

in $\mathbb{Z}/n\mathbb{Z}$

Dieses System kann nun wie üblich gelöst werden.

Bsp: $x \equiv 5 \mod 33,\ x \equiv 8 \mod 39$

($\Rightarrow 5 \equiv 2 \mod 3,\ 8 \equiv 2 \mod 3 \Rightarrow c = 2$

$\Rightarrow$ Ansatz: $x = 2 + 3y$)

$2 + 3y \equiv 5 \mod 33 \wedge 2 + 3y \equiv 8 \mod 39$

$\Leftrightarrow 3y \equiv 3 \mod 33 \wedge 3y \equiv 6 \mod 39$

$\Leftrightarrow y \equiv 1 \mod 11 \wedge y \equiv 2 \mod 13$

Lösung: $y = 67$ $\Rightarrow$ Lösung des ursprüngl. Systems: $2 + 3 \cdot 67 = 203$

H24 T2 A2 (a) ges: $a \in \{0, 1, \ldots, 82\}$

mit $50^{247} \equiv a \mod 83$

Gesucht ist die eindeutig bestimmte Repr.

in $\{0, 1, \ldots, 82\}$ von $\overline{50}^{247} \in \mathbb{Z}/83\mathbb{Z}$.

83 ist Primzahl $\Rightarrow (\mathbb{Z}/83\mathbb{Z})^\times$ ist zyklisch

von Ordnung 82 $\overline{50} \in (\mathbb{Z}/83\mathbb{Z})^\times \Rightarrow$

$\overline{50}^{82} = \overline{1}$ $\quad 247 = 3 \cdot 82 + 1 \Rightarrow$

$\overline{50}^{247} = \overline{50}^{3 \cdot 82 + 1} = \left(\overline{50}^{82}\right)^3 \cdot \overline{50} =$

$\overline{1}^3 \, \overline{50} = \overline{50} \Rightarrow$ Die gesuchte Zahl

ist $a = 50$.

(b) Nach dem Satz von Wilson gilt

$(p-1)! \equiv -1 \bmod p$ für jede Primzahl p

ges.: $a \in \{0, 1, \ldots, 100\}$ mit $98! \equiv a \bmod 101$

[$p = 101$ Primzahl $\Rightarrow 100! \equiv -1 \bmod 101$]

[$100! = 100 \cdot 99 \cdot 98!$]

Da 101 eine Primzahl ist, ist $\mathbb{Z}/101\mathbb{Z}$ ein Körper. In diesem Körper gilt nach dem Satz von Wilson

$$100! + 101\mathbb{Z} = -1 + 101\mathbb{Z} \quad \rightsquigarrow$$

$$(100 + 101\mathbb{Z}) \cdot (99 + 101\mathbb{Z}) \cdot (98! + 101\mathbb{Z}) = -1 + 101\mathbb{Z} \quad \rightsquigarrow$$

$(-1+101\mathbb{Z})\cdot(-2+101\mathbb{Z})\cdot(98!+101\mathbb{Z}) = -1+101\mathbb{Z}$

$\cdot(-1+101\mathbb{Z})$

$\Leftrightarrow \quad (-2+101\mathbb{Z})\cdot(98!+101\mathbb{Z}) = 1+101\mathbb{Z}$

$101 \nmid (-2) \Rightarrow -2+101\mathbb{Z} \in (\mathbb{Z}/101\mathbb{Z})^\times$

$\Rightarrow 98!+101\mathbb{Z} = (-2+101\mathbb{Z})^{-1}$

$2\cdot 50 \equiv -1 \bmod 101 \Rightarrow$

$(-2)\cdot 50 \equiv 1 \bmod 101 \Rightarrow$

$(-2+101\mathbb{Z})^{-1} = 50+101\mathbb{Z}$

Also ist $a=50$ die gesuchte Zahl.

(c) Sei φ die Eulersche φ-Funktion. Beweisen Sie, oder widerlegen Sie durch ein Gegenbeispiel (i) $n>m \Rightarrow \varphi(n)>\varphi(m)$ $\forall n,m\in\mathbb{N}$

(ii) $\varphi(2n)\geq\varphi(n)$ $\forall n\in\mathbb{N}$

(iii) $\varphi(n)\mid\varphi(n^2)$ $\forall n\in\mathbb{N}$

[Erinnerung: $m, n \in \mathbb{N}$ teilerfremd $\Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$, p Primzahl, $r \in \mathbb{N} \Rightarrow \varphi(p^r) = p^{r-1}(p-1)$]

zu (i) Aussage ist falsch, Bsp. $6 > 3$, aber $\varphi(6) = 2 = \varphi(3)$

zu (ii) Sei $n \in \mathbb{N} \Rightarrow \exists m \in \mathbb{N}$ ungerade, $r \in \mathbb{N}_0$ mit $n = 2^r m$ 2^r und m teilerfremd. ebenso 2^{r+1} und $m \Rightarrow \varphi(2n) = \varphi(2^{r+1} m) = \varphi(2^{r+1})\varphi(m)$

$= 2^r \cdot \varphi(m)$

1. Fall: $r = 0 \Rightarrow \varphi(2n) = 2^r \varphi(m) = \varphi(m) = \varphi(n)$

2. Fall: $r \geq 1 \Rightarrow \varphi(2n) = 2^r \varphi(m) \geq 2^{r-1} \varphi(m) =$

$\varphi(2^r m) = \varphi(n)$

zu (iii) Beweise die Aussage zunächst in dem Fall $n = p^r$, wobei p Primzahl und $r \in \mathbb{N}$ ist

$$\varphi(n) = \varphi(p^r) = p^{r-1}(p-1).$$

$$\varphi(n^2) = \varphi(p^{2r}) = p^{2r-1}(p-1)$$

Wegen $r-1 \leq 2r-1$ ist $\varphi(n)$ Teiler von $\varphi(n^2)$

allgemeiner Fall: Sei $n \in \mathbb{N}$ beliebig und $n = \prod_{i=1}^{s} p_i^{r_i}$ mit $s \in \mathbb{N}_0$, $p_1, \dots, p_s$ verschiedene Primzahlen, $r_1, \dots, r_n \in \mathbb{N}$. Da $p_1^{r_1}, \dots, p_s^{r_s}$ paarweise teilerfremd sind, gilt $\varphi(n) \overset{(*1)}{=} \prod_{i=1}^{s} \varphi(p_i^{r_i})$

Primzahlen, $r_1, \dots, r_n \in \mathbb{N}$. Da $p_1^{r_1}, \dots, p_s^{r_s}$

Ebenso erhält man $\varphi(n^2) \overset{(*_2)}{=} \prod_{i=1}^{s} \varphi\left((p_i^{r_i})^2\right)$

Auf Grund des 1. Falls gilt $\varphi(p_i^{r_i}) \mid \varphi((p_i^{r_i})^2)$ für $1 \le i \le s$. Daraus folgt wegen $(*_1)$ und $(*_2)$ auch $\varphi(n) \mid \varphi(n^2)$.

Übung: H09T1A1

F18T2A4 (Übung: H13T3A5)

(a) Bestimmen Sie alle $n \in \mathbb{N}_0$ mit der Eigenschaft, dass $2^n + 3$ bzw. $2^n + 5$ durch 3, 5, 7 bzw. 13 teilbar sind.

$= 2^r \cdot \varphi(m)$

1. Fall: $r = 0 \Rightarrow \varphi(2n) = 2^r \varphi(m) = \varphi(m) = \varphi(n)$

(i) Teilbarkeit durch 3: Sei $n \in \mathbb{N}_0$.

Es gilt die Äquivalenz $3 \mid (2^n + 3) \iff 3 \mid 2^n$

$\iff 3 \mid 2$ Also ist dies für kein $n \in \mathbb{N}_0$ erfüllt.

3 Primzahl

$3 \mid (2^n + 5) \iff 2^n + 5 \equiv 0 \bmod 3 \iff$

$2^n \equiv -5 \equiv 1 \bmod 3 \iff \bar{2}^n = \bar{1}$ in $\mathbb{Z}/3\mathbb{Z}$

$\iff \bar{2}^n = \bar{1}$ in $(\mathbb{Z}/3\mathbb{Z})^\times$ Wegen $\bar{2}^1 \neq \bar{1}$ mod

$\bar{1} \in (\mathbb{Z}/3\mathbb{Z})^\times$

$\bar{2}^2 = \bar{1}$ ist $\bar{2}$ in $(\mathbb{Z}/3\mathbb{Z})^\times$ ein Element der Ordnung 2.

Also ist die Bedingung für alle geraden $n \in \mathbb{N}_0$ erfüllt

lii) Teilbarkeit durch 5:

$5 \mid (2^n+3) \Leftrightarrow 2^n \equiv -3 \bmod 5 \Leftrightarrow$

$2^n \equiv 2 \bmod 5 \Leftrightarrow \bar{2}^n = \bar{2}$ in $\mathbb{Z}/5\mathbb{Z}$

$\Leftrightarrow \bar{2}^{n-1} = \bar{1}$ in $\mathbb{Z}/5\mathbb{Z}$ (*)

$\bar{2} \in (\mathbb{Z}/5\mathbb{Z})^\times$

Wegen $\bar{2}^2 = \bar{4} \neq \bar{1}$, $\bar{2}^4 = \bar{4}^2 = \bar{16} = \bar{1}$ ist

$\operatorname{ord}(\bar{2}) = 4$ in $(\mathbb{Z}/5\mathbb{Z})^\times$. Also ist (*) äquivalent zu $4 \mid (n-1)$, also zu $n \equiv 1 \bmod 4$.

$5 \mid (2^n+5) \Leftrightarrow 2^n + 5 \equiv 5 \bmod 5 \Leftrightarrow$

$2^n \equiv 0 \bmod 5 \Leftrightarrow 5 \mid 2^n \overset{5 \text{ Primz}}{\Leftrightarrow} 5 \mid 2$

Dies ist für kein $n \in \mathbb{N}$ erfüllt

(iii) Teilbarkeit durch 7:

$7 \mid (2^n+3) \iff 2^n \equiv -3 \equiv 4 \bmod 7 \iff$

$\iff \bar{2}^n = \bar{2}^2$ in $(\mathbb{Z}/7\mathbb{Z})^\times \iff \bar{2}^{n-2} = \bar{1}$ in $(\mathbb{Z}/7\mathbb{Z})^\times$

Wegen $\operatorname{ord}(\bar{2}) = 3$ in $(\mathbb{Z}/7\mathbb{Z})^\times$ ist dies äquivalent zu $n \equiv 2 \bmod 3$.

$7 \mid (2^n+5) \iff 2^n \equiv -5 \equiv 2 \bmod 7 \iff$

$\bar{2}^n = \bar{2}^1$ in $(\mathbb{Z}/7\mathbb{Z})^\times \iff n \equiv 1 \bmod 3$

(iv) Teilbarkeit durch 13:

$13 \mid (2^n+3) \iff 2^n \equiv -3 \equiv 10 \bmod 13 \iff$

$\bar{2}^n = \overline{10}$ $\left[\bar{2}^2 = \bar{4},\ \bar{2}^3 = \bar{8},\ \bar{2}^4 = \bar{3},\ \bar{2}^5 = \bar{6}\right.$

$\left. 2^6 = \overline{12} = -\bar{1} \Rightarrow \bar{2}^{10} = \bar{2}^4 \bar{2}^6 = \bar{3} \cdot (-\bar{1}) = -\bar{3} = \overline{10} \right] \iff \bar{2}^n = \bar{2}^{10}$ (*2)

Wegen $\bar{2}^6 = -\bar{1} \neq \bar{1}$ und $\bar{2}^{12} = (\bar{2}^6)^2 = (-\bar{1})^2 = \bar{1}$ gilt $\operatorname{ord}(\bar{2}) = 12$ in $(\mathbb{Z}/13\mathbb{Z})^\times$. Also ist die Bed.$^{(*_2)}$ äquivalent zu $n \equiv 10 \bmod 12$.

$13 \mid (2^n + 5) \iff 2^n \equiv -5 \equiv 8 \bmod 13$

$\iff \bar{2}^n = \bar{2}^3$ in $(\mathbb{Z}/13\mathbb{Z})^\times \iff$ (ord$(\bar{2}) = 12$)

$n \equiv 3 \bmod 12$.

(b) Bestimmen Sie alle $n \in \mathbb{N}_0$ mit der Eigenschaft, dass $2^n + 3$ und $2^n + 5$ beides Primzahlen sind.